UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No.

FILED UNDER SEAL

COMPLAINT

Plaintiff MICROSOFT CORPORATION ("Microsoft") hereby complains and alleges that JOHN DOES 1-2 (collectively "Defendants"), have illegally created and are using for criminal purposes a global network of interconnected computers knows as the "Necurs Botnet" or "Necurs." Necurs is comprised of computing devices connected to the Internet that Defendants have infected with malicious software (referred to as "malware"), including banking Trojans, spamware, and ransomware. The Necurs botnet is an extremely scaled infrastructure capable of sending a massive volume of spam and is one of the largest bodies of infrastructure in the spam email threat ecosystem. To date, Necurs has infected at least 9 million victim computers. Defendants have used and will continue to use Necurs to send spam email, install malicious software, steal financial account information, funds and personal information from millions of individuals. Unless enjoined and held accountable, Defendants will continue to use Necurs to engage in this harmful activity. Defendants control Necurs through a command and control infrastructure (the "Necurs Command and Control Domains") hosted and and operating through the Internet domains set forth at **Appendices A** and **B** to this Complaint. Microsoft alleges as follows:

NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.* (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) conversion; (8) unfair competition; and (9) unjust enrichment. Microsoft seeks injunctive and other equitable relief and damages against Defendants, to prevent Defendants from engaging in these violations of law and disabling the Necurs Command and Control Domains. Defendants, through their illegal activities involving Necurs, have caused and continue to cause irreparable injury to Microsoft, its customers and licensees, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. John Doe 1 controls Necurs and the Necurs Command and Control Domains in furtherance of conduct designed to cause harm to Microsoft, its customers and licensees, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

4. John Doe 2 controls Necurs and the Necurs Command and Control Domains in furtherance of conduct designed to cause harm to Microsoft, its customers and licensees, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

5. Third parties VeriSign, Inc., VeriSign Information Services, Inc., and VeriSign Global Registry Services (collectively, "VeriSign") are the domain name registries that oversee the registration of all domain names ending in ".com," ".net," ".cc," and ".tv" and are located at 12061 Bluemont Way, Reston, Virginia 20190.

6. Third party Public Interest Registry is the domain name registry that oversees the registration of all domain names ending in ".org," and is located at 1775 Wiehle Avenue, Suite 100, Reston, Virginia 20190.

7. Third party Afilias Limited c/o Afilias USA, Inc. is the domain name registry that oversees the registration of all domain names ending in ".pro" and is the domain name registry backend provider for the domains ending in .me, .mn and .sc is located at 300 Welsh Road, Building 3, Suite 105, Horsham, Pennsylvania 19044.

8. Third parties Neustar, Inc., is the domain name registry that oversees the registration of all domains ending in ".biz" and ".us." Neustar, Inc. is located at 21575 Ridgetop Circle, Sterling, Virginia 20166.

9. Third parties Neustar, Inc. and .CO Internet S.A.S. are the domain name registry backend provider and domain name registry that oversee the registration of all domains ending in ".co." Neustar, Inc. is located at 21575 Ridgetop Circle, Sterling, Virginia 20166 and .CO Internet S.A.S, World Trade Center Calle 100 No. 8 A – 49 Torre B of. 507, Bogotá, Colombia

10. Third party ICM Registry LLC is the domain name registry that oversees the registration of all domain names ending in ".xxx" and is located at PO Box 30129, Palm Beach Gardens Florida 33420.

11. Set forth in **Appendices A and B** are the identities of and contact information for third party domain registries that control the domains used by the Defendants.

12. On information and belief, John Does 1-2 jointly own, rent, lease, or otherwise have dominion over the Necurs Command and Control Domains and related infrastructure and through those control and operate Necurs. Microsoft will amend this complaint to allege the Doe Defendants' true names and capacities if and when ascertained. Microsoft will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

13. Microsoft is informed and believes and thereupon alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Defendants.

14. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-2 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions that each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of the other Defendant, as set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the other Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendant.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violations of The Computer Fraud and Abuse

Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, intentional interference with contractual relationships, unjust enrichment, unfair competition, and conversion pursuant to 28 U.S.C. § 1367.

16. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants have conducted business in the Eastern District of New York and have utilized instrumentalities located in the Eastern District of New York to carry out the acts of which Microsoft complains.

17. Defendants have affirmatively directed actions at New York and the Eastern District of New York by directing malicious computer code at the computers of individual users located in New York and the Eastern District of New York, by attempting to infect and in fact infecting those computing devices with the malicious code to make the computing devices part of the Necurs botnet, by directing malicious computer code and instructions to Microsoft's Windows operating system and computers of individual users and entities located in New York and the Eastern District of New York, in order to compromise the security of those systems, to install malicious software on those systems and to steal funds and resources from and through those computers, all to the grievous harm and injury of Microsoft, its customers and licensees, and the public. **Figures 1, 2** and **3**, below, depict the geographic location of computer devices in and around the Eastern District of New York, against which Defendants are known to have directed malicious code, attempting to or in fact infecting those devices, thereby enlisting them

into the Necurs botnet.

Figure 1

Figure 2

Figure 3

18. Defendants use certain of the Necurs Command and Control Domains to communicate with and control the Necurs-infected computing devices located in this judicial district that Defendants communicate with, control, steal from, update, and maintain. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through computing devices located in the Eastern District of New York, thereby injuring Plaintiff, its customers, and others in the Eastern District of New York and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

19. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Microsoft's Services and Reputation

20. Microsoft® is a provider of the Windows® operating system. Microsoft has invested substantial resources in developing high- quality products and services. Due to the high

quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well- recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft and Windows. Copies of the trademark registrations are attached as **Appendix C** to this Complaint.

Computer "Botnets"

21. A "botnet" is a collection of individual computing devices infected with malware that allows communication among those computing devices and centralized or decentralized communication with server computers providing control instructions. A botnet network may be comprised of hundreds of thousands and sometimes millions, as in this case, of infected computing devices. The individual computing devices in a botnet often belong to users who have unknowingly downloaded or been infected by the malware. A user's computing device, for example, may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment, or downloads a document that contains hidden malware. In each instance where a Necurs malware is downloaded and successfully executed on the user's computing device, it causes that device to become part of the Necurs botnet. Once part of a botnet, the user's computing device is capable of sending and receiving communications, code, and instructions to and from other botnet computers.

22. Malicious actors leverage the computer powers and Internet-accessibility of the infected computers to target and infiltrate additional computers.

23. Many botnets are controlled through a set of specialized server computers referred to as "command and control servers." The command and control servers are often wholly under the control of the botnet creators. These may have specialized functions, such as sending control instructions to infected computing devices and uploading stolen information from them.

24. Criminal organizations and individual cybercriminals usually create, control, maintain, and propagate botnets in order to carry out misconduct that harm others' rights. Cybercriminals factor the use of botnets for many illegal activities because botnets support a wide range of illegal conduct, are difficult for security experts to disable or eradicate, and use a variety of networks and firewalls to conceal the identities of the malefactors controlling them. The controllers of a botnet will use an infected computing device for a variety of illicit purposes, unknown to the end user. A computing device in a botnet, for example, may be used to:

a. Carry out theft of money, credentials, or other sensitive information or engage if fraud, computing device intrusions, or other misconduct;

b. Anonymously send unsolicited bulk email or other electronic messages without the knowledge or consent of the individual user who owns the compromised computing device;

c. Deliver further malware to infect other computing devices; or

d. "Proxy" or relay Internet communications originating from other computer devices, in order to obscure and conceal the true source of those communications.

25. Botnets provide a very efficient means of controlling a large number of computer devices for illegal purposes and a means of targeting any illicit action against the

contents of those devices, the users of those devices, or against computing devices and networks connected to the Internet.

NECURS

26. Plaintiff brings this action to stop Defendants from harming Plaintiff, its customers, and the public, through the Necurs Command the Control Domains, which are central to the Necurs botnet's illegal operation.

27. Necurs is a prolific and globally diverse spam and malware distribution botnet. The Necurs botnet has infected over nine million end user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. These infected computers exist around the world and are a substantial and robust delivery mechanism for phishing attacks, distributing ransomware, financial target malware, and other criminally motivated spam email campaigns.

28. Necurs is used in a variety of illegal activities and is known to have distributed the some of the world's most sophisticated malware, including Game Over Zeus, Dridex, Locky and Trickbot. Necurs arrives into a victim's system by being downloaded by other malware, through either spammed email attachments or malicious advertisements. Once on a system, Necurs utilizes its kernel mode rootkit capabilities to disable a large number of security applications, including Windows Firewall, both to protect itself and other malware on the infected system.

29. Once the Necurs malware infects a new victim computing device, it contacts a command and control computer over the Internet from which it begins to receive instructions and additional malware modules. This effectively places the infected computer under the command of Defendants, the operators of the botnet.

30. The user of the infected computer is unaware of Necurs' activity as Defendants have designed Necurs to hide itself and its unlawful activity on infected computing devices in part by disabling the security defenses of the user's device. The operating system still purports to be Windows, but, in fact, Necurs has corrupted and thereby converted the Windows operating system into instruments of fraud aimed directly at the user of the computing device. The typical user is unaware of Defendants intrusion, theft, surveillance and control of their computing device.

31. Necurs is designed as a "pay-per-install" criminal business enterprise that compensates hackers who distribute the Necurs malware onto additional computers. The user of the infected computer is likewise unaware that Necurs' malware is designed to use the infected computers to spread the malware to additional victim computers, expanding the scope of the botnet. The Necurs code contains code that transforms the infected computer into a spam email distribution, a distributor of fraud and ransomware and a target of theft of funds and information. For example, a single computer infected with Necurs malware is capable of sending approximately 3.6 million spam emails to approximately 40 million people over 58 days.

The Necurs Botnet's Infrastructure

32. Like other botnets, the Necurs botnet is comprised of a large number of victim computers that have been infected by the Defendants with the Necurs malware. Further, the Necurs botnet includes computers that have a "command and control" purpose. These command and control computers are utilized by the Defendants to transfer command and control instructions to the infected victim computers, in order to maintain control over the operation of those victim computers and to carry out the numerous types of harmful activities described more fully later in this declaration.

Infected Victim Computers In The Necurs Botnet

33. The infected victim computers in the Necurs botnet are essentially the workers of the Necurs botnet, performing the day-to-day illegal activity. For example, Defendants use these computers to send spam email, encrypt the computers with ransomware and demand a ransom or install financial theft malware which enables them to ultimately steal money directly from these individuals' bank accounts, as well as to steal personal information from the owners of the infected computers and engage in other malicious activity directed at these victims.

34. The Necurs malware also serves an additional purpose, to perpetuate additional malicious actions and infiltrate even more victim computers. The Necurs botnet infects victim computers with the following malware: Game Over Zeus (financial theft malware), Locky (ransomware), Dridex (ransomware), and a DDoS module (a module designed to launch distributed denial of service attacks on other computers). Each of these secondary malware infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow remote control by other cybercriminals, and allowing yet further sets of malware to be downloaded onto the computing device. All of these malware variants are designed to attack computing devices running Microsoft Windows operating systems and may themselves be connected to other criminal botnet infrastructure beyond Necurs receiving additional commands.

The Necurs Command and Control Computers

35. As mentioned, after the Necurs malware infects a victim computing device, it connects over the Internet to one of its pre-programmed command and control servers. These command and control servers are specialized servers and/or software that Defendants use to send commands to control the Necurs botnet's infected victim computers. The command and control

computers send the most fundamental instructions, updates, and commands, and overall control of the botnets is carried out from these computers. To create the command and control servers, Defendants set up accounts with web-hosting providers—i.e., companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities. By contacting a command and control server, the Necurs malware can receive updated commands and modules from and communicate with the Defendants

36. The Defendants are able to send and receive communications between their command and control servers and the infected victim computers in the Necurs botnet, by means of three different communication channels. **Figure 4** below illustrates these communication channels of the Necurs botnet.

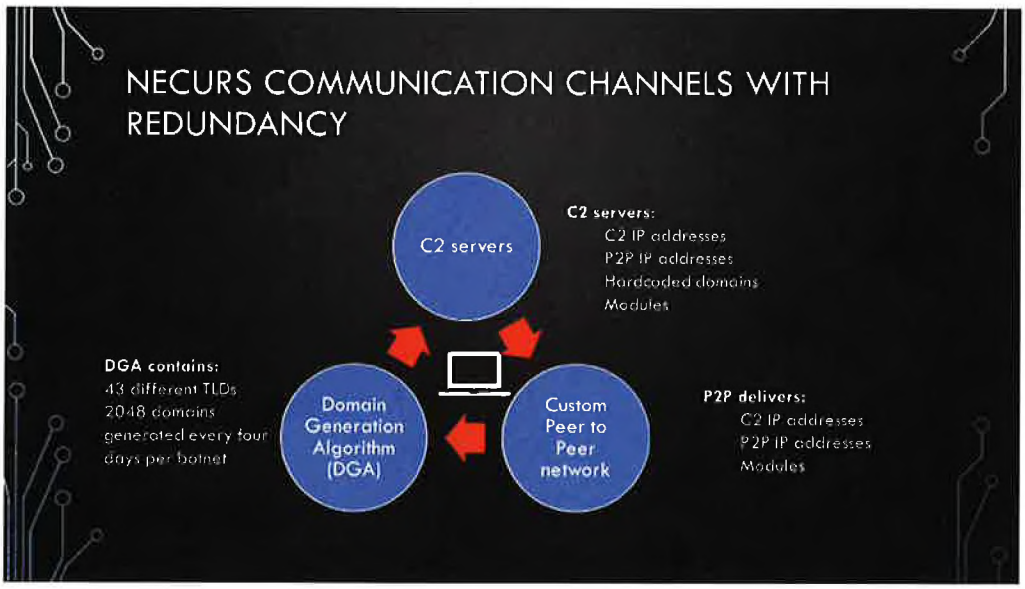


Figure 4

37. First, the primary communication between victim and Command and Control (C2) is through (1) a set of IP addresses controlled by Defendants, and used via IP address to IP address communications utilizing Hypertext Transfer Protocol ("HTTP"), and (2) a "hardcoded"

domain that is preprogrammed into the Necurs malware. The hardcoded domain is set forth at **Appendix A** to this complaint. Second, the C2 IP addresses are distributed throughout the botnet via direct download from C2 server or through Peer to Peer (P2P) network which is comprised of other Necurs infected victim computers. Third, the botnet also uses Internet domains generated by a Domain Generation Algorithm ("DGA"), as a backup communications channel. The DGA domains are set forth at **Appendix B** to this complaint.

38. The primary communication channel between infected victim computers and the command and control servers are either particular IP addresses controlled by Defendants (which are reached by IP address to IP address communications utilizing Hypertext Transfer Protocol or "HTTP") or a particular domain name that is preprogramed into the Necurs malware (referred to as "hardcoded" domain), which are set forth at **Appendix A**.

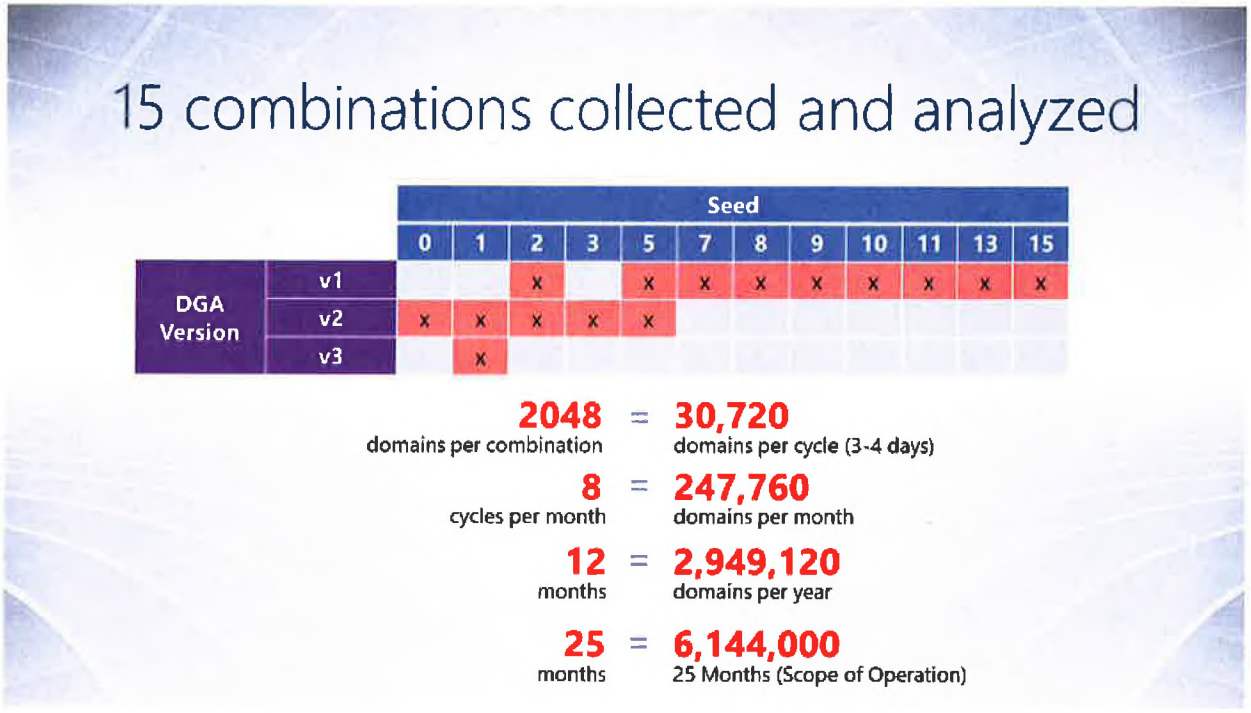
39. A secondary communication channel between infected victim computers and the command and control computers is comprised of IP addresses distributed throughout the botnet via direct download from command and control servers or through a "peer-to-peer" network (sometimes abbreviated as "P2P") which is comprised of other Necurs-infected victim computers. This communication level ensures information can be continuously transmitted between the command and control servers and the infected computers if the primary communication means is disrupted. Both cryptographically signed P2P messages and TCP and UDP protocols are deployed to ensure this backup channel remains active to perpetuate Defendants' fraud and malicious actions.

40. Necurs also uses internet domain names generated by a Domain Generation Algorithm ("DGA") that is contained within the Necurs malware on infected victim computers as a "fallback" communication channel. When all of the other command and control

communications channels of the Necurs botnet are disrupted, and Defendants cannot use them to communicate with the infected victim computers, then the Necurs malware on the infected victim computers detects that fact and reverts to the DGA in order to create domains as a "fallback" backup communication channel for the botnet. These domains are set forth in **Appendix B**.

41. DGAs are algorithms that rely upon a pseudorandom schema to generate a large number of domain names that can be used as rendezvous points with the command and control servers. In other words, the Necurs malware creates lists of domains and attempts to connect to them to receive command and control instructions, with the expectation that the Defendants will register some or all of those domains and be able to re-exert control over the botnet. The domains are pseudorandomly generated strings of letters or numbers (for example, "iioxtbyqnuajqftp[.]TLD" etc.). They do not have any commercial value and do not represent any real words.

42. The purpose of the DGA is to create lists of domains that are not yet registered and which are not likely at all to be registered by any party. In this way, after losing control of the botnet, the Defendants can register these domains, knowing that the infected victim computers will eventually be reaching out to those domains seeking instructions. The large number of potential rendezvous points makes it increasingly difficult to effectively shut down botnets, since the infected computers will attempt to contact some of these new domain names every day to receive updates or commands. Microsoft has identified a staggering 6,144,000 prospective DGA command and control domains, across the 15 variants of the botnet, which the Necurs botnet can deploy at any moment, once all of the IP address infrastructure and hardcoded domain infrastructure is disrupted.



43. Given that the primary IP address-based command and control infrastructure is not in use, given the current operational state of the Necurs botnet, and given collaboration between Microsoft and its private and public partners, Microsoft has prepared means to disable and disrupt the IP address-based command and control infrastructure of the Necurs botnet. Thus, it is necessary to disable the "hardcoded" domain and the fallback "DGA" domains, in order to disrupt the Necurs botnet. Disablement of these domains is the goal of the relief sought in the instant action.

Harm To Microsoft And Microsoft's Customers

44. The Necurs malware infection harms Microsoft, its customers, and the public by damaging the customers' computing devices and the software installed on those devices licensed from Microsoft, including degrading the integrity of the computers and the operating system, intruding into those devices, disabling some of those systems' antivirus software, and carrying out malicious actions from those computers and directed toward the owners of those computers.

During the infection of a user's device, the Necurs malware makes changes at the deepest and most sensitive levels of the device's operating system. Additionally, it makes fundamental changes at the level of the Windows registry. Microsoft's customers whose computing devices are infected with the malicious software are damaged by these changes to Windows, which alter the normal and approved settings and function of the user's operating system, destabilize it, and forcibly draft the customers' devices into the botnet. Necurs severely damages the computing devices it infects, making low-level changes to the operating system and, with respect to Windows 7, degrades the primary security defense of most computing devices – the antivirus software – by blocking the computing device from getting anti-virus software updates. This functionality, however, is not possible on a computing device running an updated Windows 7, with updated antivirus software, and in Windows 10, a more recent version of the Windows operating system. As a result, for devices using an outdated Windows 7 without updated antivirus protections, Necurs not only cripples the security mechanism that might result in removal of Necurs from the computing device, it may leave victim's computing devices exposed to against many other types of malware.

45. Once a computing device is infected, the Windows operating system cease to operate normally and are transformed into tools of deception and theft. But Windows still bears Microsoft's trademarks. This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks. Trademark registrations for the marks infringed by Defendants are attached to this complaint as **Appendix C**.

46. Customers who experience degraded performance of Microsoft's product may attribute such poor performance to Microsoft, causing extreme damage to Microsoft's brands and trademarks and goodwill associated there with. Even customers who eventually come to learn

their computing devices are infected with malware may incorrectly attribute the infection to vulnerabilities in Microsoft's products, because many customers are unaware that they have fallen prey to Defendants' attacks.

47. Moreover, as a provider of Windows, Microsoft devotes significant computing and human resources to combating Necurs and other malware infections and helping customers determine whether or not their computing devices are infected and, if so, cleaning them. Not only does Microsoft expend resources in helping users combat Necurs, these efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers. Microsoft, as a provider of the Windows operating systems, must also incorporate security features in an attempt to stop installation of the Necurs malware and other malicious software that is distributed by the Necurs botnet. Microsoft has expended significant resources to investigate and track the Necurs Defendants' illegal activities and to counter and remediate the damage caused by the Necurs botnet to Microsoft, its customers, and the general public.

48. Necurs also inflicts severe harm on individuals whose computing devices it infects. Once a computing device is infected with Necurs, Defendants can use the victims' computers to send spam email or to deliver other malware that, among other things, enables Defendants to take control of victims' computers and extort money from them, steal their online banking credentials, or constantly monitor the online activities of its unknowing victims and also send commands and instructions to the infected computing device to control it surreptitiously. Defendants' primary goal, as made evident by the Necurs' functionality, is to propagate spam email, deliver financial theft malware, deliver ransomware, enable attacks against other computers and to steal online account login IDs, passwords, and other personal identifying

information.

49. One of the principal activities of the Necurs malware is to cause victim computers to send massive amounts of spam email to other victims on the Internet. The Necurs botnet delivers spam by converting a victim computer into an email server that is capable of sending a vast amount of emails per day, as indicated above. The victim computer receives specialized templates of the spam email that it is supposed to send, as well as target email addresses to which the spam email is sent.

50. Necurs is capable of sending a massive volume of spam and is one of the largest bodies of infrastructure in the spam email threat ecosystem. One single infected Necurs computer is capable of sending a total of 3.8 million spam emails to over 40.6 million potential victims over a 58 day period.

51. The Necurs malware is designed to enable *other* criminal actors to transmit additional types of malware to infect devices in the Infected Tier. Each of these secondary malware infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing yet further sets of malware to be downloaded onto the computing device. All of these malware variants are designed to attack computing devices running Microsoft Windows operating systems and may themselves be connected to other criminal botnet infrastructure beyond Necurs receiving additional commands.

52. To carry out the intrusion into computing devices, Defendants cause the Necurs malware to make repeated copies of Microsoft's trademarks onto computing devices, in the form of file names, domain names, target names, and/or registry paths containing the trademarks "Microsoft" and "Windows." These uses of Microsoft's trademarks are designed to cause the

intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not.

53. There is a serious risk that customers may move from Microsoft's products and services because of such activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

54. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 53 above.

55. Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission of information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

56. Defendants' conduct involved interstate and/or foreign communications.

57. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000.

58. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

59. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

60. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 59 above.

61. Microsoft's Windows operating system and Microsoft's customers' computers running such software are facilities through which electronic communication service is provided to Microsoft's users and customers.

62. Defendants knowingly and intentionally accessed the Windows operating system and Microsoft's customers' computers running such software without authorization or in excess of any authorization granted by Microsoft or any other party.

63. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered authorized access to, wire electronic communications transmitted via Microsoft's Windows operating system and computers running such software.

64. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

65. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Trademark Infringement under the Lanham Act–15 U.S.C. § 1114 *et seq.*

66. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 65 above.

67. Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft and Windows.

68. The Necurs botnet generates and uses unauthorized copies of Microsoft's

trademarks in corrupted and sabotaged versions of the Windows operating system, including through the software opening from and through the Necurs Command and Control Domains. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system.

69. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act.

70. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

71. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

72. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq*.

FOURTH CLAIM FOR RELIEF

False Designation of Origin under the Lanham Act–15 U.S.C. § 1125(a)

73. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 72 above.

74. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

75. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products that are likely to

cause confusion, mistake, or deception.

76. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

77. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

78. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Trademark Dilution under the Lanham Act–15 U.S.C. § 1125(c)

79. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 78 above.

80. Microsoft's trademarks are famous marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

81. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Microsoft's trademarks.

82. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

83. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

84. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 83 above.

85. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

86. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers.

87. Defendants' actions in operating Necurs result in unauthorized access to Microsoft's Windows operating system and the computers on which such programs and services run, and result in unauthorized intrusion into those computers.

88. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

89. Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software.

90. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

91. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Conversion

92. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 91 above.

93. Microsoft owns all right, title, and interest in its Microsoft and Windows, Outlook, Windows Live, Hotmail, OneDrive and Office 365 software and services. Microsoft licenses its software and services to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows, Outlook, Windows Live, Hotmail, OneDrive and Office 365 software and services.

94. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and/or computer software from a computer or computer network.

95. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

96. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Unfair Competition

97. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 96 above.

98. The acts of Defendants complained of herein constitute unfair competition at the expense of Microsoft in violation of the common law. Defendants used, without authorization or license, Microsoft's trademarks in a deceptive manner likely to mislead customers into falsely believing Defendants' conduct was that of Microsoft.

99. Defendants' actions have irreparably injured Microsoft by tarnishing its reputation with its customers. Microsoft has cultivated good-will with customers at great expense

over many years.

NINTH CLAIM FOR RELIEF

Unjust Enrichment

100. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 99 above.

101. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft in violation of the common law. Defendants used, without authorization or license, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants. In this manner, Microsoft conferred a benefit on the Defendants.

102. Defendants retained the benefit of and profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

103. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

104. Retention by the Defendants of the benefit and profits they derived from their malfeasance would be inequitable and unjust.

105. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

106. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays that the Court:

1. Enter judgment in favor of Microsoft and against the Defendants.

2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice, and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter a preliminary and permanent injunction giving Microsoft control over the domains used by Defendants to cause injury and enjoining Defendants from using such instrumentalities.

5. Enter judgment awarding Microsoft actual damages from Defendants adequate to compensate Microsoft for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

6. Enter judgment disgorging Defendants' profits.

7. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proven at trial.

8. Enter judgment awarding attorneys' fees and costs, and order such other relief that the Court deems just and reasonable.

Dated: March 5, 2020

Respectfully submitted,

KAYVAN M. GHAFFARI

Gabriel M. Ramsey (*pro hac vice* application pending)
Kayvan M. Ghaffari
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com

Richard Domingues Boscovich (*pro hac vice* application pending)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.